

**FOR IMMEDIATE RELEASE**  
**March 15, 2005**

**CONTACT: Tara McGuinness**  
**(202) 225-2836**

**Opening Statement of Representative Edward J. Markey (D-MA)**  
**House Energy and Commerce Committee**  
**Subcommittee on Commerce, Trade, and Consumer Protection**  
**“Protecting Consumer’s Data: Policy Issues Raised by ChoicePoint”**  
**Tuesday, March 15, 2004**

Thank you, Mr. Chairman for calling today’s hearing.

Americans take privacy seriously. We guard our credit cards by carefully returning them to our wallets, we keep our mortgage records and social security cards and personal documents locked up. How would consumers feel if they discovered that while they take extra precautions to guard their personal information, their names, social security numbers, tax records, credit histories and employment documents were piled high into wheelbarrows and baskets and sold to the highest bidder in a bustling market place that is as frenetic and unregulated as the streets of Bombay?

“RIGHT HERE, GET YOUR SOCIAL SECURITY NUMBERS!!!!”

“MEEEEEEEDICAL RECORDS, EMPLOYMENT HISTORY—CHEAPER BY THE DOZEN.”

How would you feel if you knew that your social security number was in some identity vendor’s suitcase of wares? You would probably feel violated.

That is exactly how two of my constituents, Kei and Karen Kishimoto felt this week when they received a letter from ChoicePoint, stating that they were among the 145,000 victims whose social security numbers and other sensitive and personal data were compromised by ChoicePoint. Kei and Karen wrote:

“We are furious that ChoicePoint has irresponsibly allowed this to happen. We have taken every precaution within our power to minimize our risk of becoming victims of identity theft – we shred sensitive documents and credit card receipts, we do not give out my social security number and credit card information unless we are sure of the credibility of the requesting source, we have changed our drivers license and insurance card from our social security numbers to random identifiers. We are outraged that there are not better safeguards in place to protect this highly sensitive data.”

Kei and Karen Kishimoto are just two of the 1,100 Massachusetts residents whose personal data was compromised when ChoicePoint allowed a group of Nigerian criminals to get access to its database. Now they, along with 145,000 consumers nationwide, are at risk of having their identities stolen and their credit and reputation damaged. They had no “Choice” about this...and that’s the point.

ChoicePoint is not the only company to have such privacy breaches; right on the heels of the ChoicePoint scandal, another 4,000 Massachusetts residents -- and some 32,000 individuals nationwide – may have had their personal data compromised by security breaches affecting customers of Lexis-Nexis’ Seisint division.

How in the world did this happen? Who are these information brokers, and how is it that they have come into possession of so much sensitive personal information about us, buying and selling our families information -- information that could, in the wrong hands, be used to harm us?

Today, the Subcommittee will be examining these issues, and I look forward to that testimony. But I hope that the Subcommittee does not limit itself to just holding oversight hearings, but that these important hearings to set the groundwork for enactment of new privacy legislation.

I have introduced two bills aimed at addressing the problems highlighted by these scandals that I hope the Subcommittee will examine.

My first bill, H.R. 1080, the "Information Protection and Security Act would subject information brokers like ChoicePoint to federal regulation by the Federal Trade Commission, and require that such brokers comply with a set of new fair information practice rules. These rules require information brokers to better secure the information in their possession, grant consumers the right to obtain access to and correct information held by the broker, require information brokers to protect information from unauthorized users, and prohibit users of an information broker from obtaining the information for impermissible or unlawful purposes. The bill's requirements will be enforceable through the FTC, which would be empowered to bring civil actions to punish and fine violators; the State Attorney's General, who could bring similar actions; and consumers,' who would be empowered to bring a private right of action.

My second bill, H.R. 1078, the "Social Security Number Protection Act," would bring a halt to unregulated commerce in Social Security numbers. This bill would make it crime for a person to sell or purchase Social Security numbers. Under the bill, the FTC would be given rulemaking authority to restrict the sale of Social Security numbers, determine appropriate exemptions, and to enforce civil compliance with the bill's restrictions. The bill would also authorize the states to enforce compliance, and provide for appropriate penalties. The sale of Social Security numbers is an outrageous form of commerce and it must be stopped. Subscribers to WestLaw, for example, can routinely download the Social Security numbers of individuals without their permission. We know that Social Security numbers are the gold standard for identity thieves, yet we have yet to act to curtail the sale of Social Security numbers for fun and profit.

I look forward to hearing the testimony of the witnesses we have assembled here today, and to working with you, Mr. Chairman, and other Members of the Subcommittee on legislation to address the privacy threat posed by current industry practices. I hope we can work together to remind these companies and American consumers that their privacy is not for sale.

For letters from constituents on ChoicePoint violations and more information on Representative Markey's work as the co-chair of the Privacy Caucus go to <http://www.house.gov/markey/>